TEORÍA DE CONJUNTOS

GUIDO URDANETA, SALVADOR PINTOS Y DANIEL FINOL

Revisado por: Suheiry Luzardo, Gustavo Meza, Luis Montiel, Adin Rangel, Jaime Soto y Claudia Vielma

ÍNDICE

Date: Febrero-2005.

1. Introducción a la Lógica

La lógica es el estudio del razonamiento; en particular, se analiza si un razonamiento es correcto. Los métodos lógicos se utilizan en matemáticas para demostrar teoremas.

Una *proposición* es una afirmación que es verdadera o falsa, pero no ambas. Por ejemplo las siguientes afirmaciones son proposiciones:

- Todos los carros tienen siete ruedas
- Para todo número entero x se cumple que si $x > 0$ entonces $2x > 0$

Las siguientes oraciones no son proposiciones:

- Continúe leyendo
- ¿De qué color te pintaste el pelo?

En lo que resta de sección, se utilizarán letras minúsculas o mayúsculas como p, q, P y Q para representar proposiciones.

1.1. Conectores Lógicos. Los conectores lógicos son símbolos que permiten construir proposiciones más complejas a partir de proposiciones existentes. Los conectores más fundamentales son la conjunción, la disyunción y la negación.

1.1.1. Conjunción. La *conjunción* de p y q, denotada $p \wedge q$, es la proposición "p y q". Esta proposición sólo es verdadera cuando tanto p como q son verdaderas. Si al menos una de las proposiciones es falsa entonces la conjunción es falsa. Esto se muestra mediante la siguiente tabla de verdad:

p	q	$p \wedge q$
F	F	F
V	F	F
F	V	F
V	V	V

1.1.2. Disyunción. La *disyunción* de p y q, denotada $p \vee q$, es la proposición "p y/o q". Esta proposición sólo es falsa cuando tanto p como q son falsas. Si al menos una de las proposiciones es verdadera entonces la disyunción es verdadera. Esto se muestra mediante la siguiente tabla de verdad:

p	q	$p \vee q$
F	F	F
V	F	V
F	V	V
V	V	V

1.1.3. Negación. La negación de p, denotada $\neg p$ o $\bar{p}$, es la proposición "no p". Si p es verdadera, entonces la negación de p es falsa y si p es falsa, la negación de p es verdadera. Esto se muestra mediante la siguiente tabla de verdad:

p	$\neg p$
F	V
V	F

1.1.4. Propiedades. A continuación algunas propiedades de la conjunción, disyunción y negación.

Theorem 1.1. *Para toda proposición p,q,r se cumple*

1. *Conmutatividad*

$$p \wedge q \text{ es equivalente a } q \wedge p$$
$$p \vee q \text{ es equivalente a } q \vee p$$

2. *Asociatividad*

$$(p \wedge q) \wedge r \text{ es equivalente a } p \wedge (q \wedge r)$$
$$(p \vee q) \vee r \text{ es equivalente a } p \vee (q \vee r)$$

3. *Idempotencia*

$$p \wedge p \text{ es equivalente a } p$$
$$p \vee p \text{ es equivalente a } p$$

4. *Distributividad*

$$p \wedge (q \vee r) \text{ es equivalente a } (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \text{ es equivalente a } (p \vee q) \wedge (p \vee r)$$

5. *Doble negación*

$$\neg\neg p \text{ es equivalente a } p$$

6. *Leyes de DeMorgan:*

$$\neg(p \wedge q) \textit{ es equivalente a } \neg p \vee \neg q$$
$$\neg(p \vee q) \textit{ es equivalente a } \neg p \wedge \neg q$$

Demostración. Todas las propiedades se demuestran fácilmente construyendo las correspondientes tablas de verdad. □

1.2. Variables. Con mucha frecuencia, es necesario construir proposiciones que dependan de objetos identificados mediante letras denominadas *variables*. Por ejemplo, si la variable x se utiliza para representar un número en algún problema podríamos estar interesados en la proposición "x es un número positivo". Aunque en ocasiones utilizaríamos una letra como p para representar esa proposición, en otras ocasiones se utilizará la notación $p(x)$ para indicar que se trata de una proposición acerca de la variable x. Esta notación nos permite construir fácilmente diferentes proposiciones para diferentes valores de x. Usando el ejemplo, $p(7)$ representaría la proposición "7 es un número positivo" y $p(a+b)$ representaría la proposición "$a+b$ es un número positivo". Se puede incluso, tener más de una variable. Por ejemplo, la proposición "x es el padre de y" podríamos representarla como $q(x,y)$ y así para cada par de valores x y y habría una proposición distinta. Las variables utilizadas en estas proposiciones se llaman *variables libres* ya que pueden tomar cualquier valor.

Con frecuencia, nos referiremos a una proposición con variables libres como una *función proposicional*.

1.3. Conectores condicionales.

1.3.1. Implicación. Considérese el siguiente razonamiento:

1. Si hoy es domingo, entonces no voy a trabajar.
2. Hoy es domingo.
3. Por lo tanto, hoy no voy a trabajar.

Las palabras "si" y "entonces" en la primera proposición hacen que la tercera proposición sea verdadera. Para representar este tipo de proposición introducimos un nuevo conector lógico, denominado *implicación*. Escribimos $p \to q$ para denotar la proposición "si p entonces q" o "p implica q" o "p es condición suficiente para q". En la proposición $p \to q$, la proposición p se conoce como hipótesis o antecedente y q como conclusión o consecuente.

En principio, la construcción de la tabla de verdad para la implicación puede no ser obvia. Podemos decir con certeza que si la hipótesis p es verdadera y la conclusión q es falsa entonces la implicación es falsa. También es razonable suponer que si p y q son verdaderas entonces la implicación es verdadera. El problema se presenta si p es falsa. Inicialmente la tabla de verdad queda como:

p	q	$p \to q$
F	F	?
V	F	F
F	V	?
V	V	V

Consideremos la siguiente proposición: "si $x > 2$ entonces $x^2 > 4$", la cual podemos representar como $P(x) \to Q(x)$, siendo $P(x)$ la proposición $x > 2$ y $Q(x)$ la proposición $x^2 > 4$. Está claro que las proposiciones $P(x)$ serán verdaderas para algunos valores de x y falsas para otros y lo mismo aplica a las proposiciones $Q(x)$. De lo que si no cabe duda es de que si se cumple $x > 2$ entonces se cumple $x^2 > 4$ y por lo tanto la implicación $P(x) \to Q(x)$ es verdadera. Supongamos que $x = 3$, en este caso $x > 2$ y $x^2 = 9 > 4$ y por lo tanto $P(x)$ y $Q(x)$ son verdaderas. Este caso corresponde a la cuarta fila de la tabla. Consideremos ahora el caso $x = 1$; en este caso $P(x)$ y $Q(x)$ son falsas, pero esto no cambia el hecho de que la implicación sigue siendo verdadera, entonces en la primera línea de la tabla debemos asignar a $p \to q$ el valor "verdadero". Por último consideremos $x = -3$; en este caso $P(x)$ es falsa y $Q(x)$ es verdadera, entonces en la tercera línea

de la tabla debemos asignar a $p \to q$ el valor "verdadero". La tabla de verdad de la implicación debe entonces escribirse de la siguiente manera:

p	q	$p \to q$
F	F	V
V	F	F
F	V	V
V	V	V

El ejemplo anterior realmente no constituye una demostración de que siempre que la hipótesis sea falsa la implicación es verdadera. La razón por la cual la hipótesis falsa hace que la implicación sea verdadera es simplemente que no se puede concluir que la implicación es falsa. En matemática, para que una proposición sea falsa debe ser posible encontrar un caso (llamado contraejemplo) que haga falsa la proposición. Si la hipótesis siempre es falsa no existe manera de encontrar tal contraejemplo y por lo tanto concluimos que la proposición no es falsa.

Nótese que la proposición $p \to q$ es equivalente a las siguientes proposiciones:

$$\neg p \vee q$$

$$\neg(p \wedge \neg q)$$

$$\neg q \to \neg p$$

Nótese también que $p \to q$ no es equivalente a $q \to p$.

1.3.2. Doble implicación. En la matemática se presenta con frecuencia el caso en que tanto $p \to q$ y $q \to p$ son verdaderas. En este caso se escribe $p \leftrightarrow q$. Esta expresión es equivalente a $p \to q \wedge q \to p$ y se lee "q si y sólo si p" o "p es condición necesaria y suficiente para q" o "p es equivalente a q". La tabla de verdad para la doble implicación es:

p	q	$p \leftrightarrow q$
F	F	V
V	F	F
F	V	F
V	V	V

Con frecuencia, la expresión "q si y sólo si p" se escribe "q ssi p".

1.4. Cuantificadores. Una proposición con variable libre $P(x)$ puede ser verdadera para algunos valores de x y falsa para otros. Con frecuencia, queremos decir que $P(x)$ es verdadera para todos los valores de x o para al menos un valor de x. Los símbolos $\forall$ y $\exists$ se denominan cuantificadores y permiten expresar estas ideas.

Para decir que $P(x)$ es verdadero para todos los valores posibles de x escribimos $\forall x P(x)$ o $\forall x(P(x))$ y leemos "para todo x, $P(x)$". El cuantificador $\forall$ se denomina *cuantificador universal*. Nótese que la proposición $\forall x(\forall y(P(x,y))$ es equivalente a $\forall y(\forall x(P(x,y))$ y en ocasiones la denotaremos como $\forall xy(P(x,y))$.

Para decir que $P(x)$ es verdadero para al menos un valor de x escribimos $\exists x P(x)$ o $\exists x(P(x))$ y leemos "existe al menos un x tal que $P(x)$" o "para algún x, $P(x)$". El cuantificador $\exists$ se denomina *cuantificador existencial*. Nótese que la proposición $\exists x(\exists y(P(x,y))$ es equivalente a $\exists y(\exists x(P(x,y))$ y en ocasiones la denotaremos como $\exists xy(P(x,y))$.

A continuación algunas propiedades de los cuantificadores:

1. $\neg\forall x(P(x))$ es equivalente a $\exists x(\neg P(x))$. Esta propiedad es sumamente importante ya que establece que si existe un contraejemplo x para una función proposicional $P(x)$ entonces queda demostrado que ésta no es verdadera para todo x y por lo tanto es falsa (aunque puede ser verdadera para muchos valores de x).
2. $\neg\exists x(P(x))$ es equivalente a $\forall x(\neg P(x))$
3. $\forall x(P(x)) \wedge \forall x(Q(x))$ es equivalente a $\forall x(P(x) \wedge Q(x))$

Notese también lo siguiente:

1. $\neg\forall x(P(x))$ no es equivalente a $\forall x(\neg P(x))$
2. $\neg\exists x(P(x))$ no es equivalente a $\exists x(\neg P(x))$
3. $\exists x(P(x)) \wedge \exists x(Q(x))$ no es equivalente a $\exists x(P(x) \wedge Q(x))$
4. $\forall x(\exists y(P(x,y))$ no es equivalente a $\exists x(\forall y(P(x,y))$

2. CONJUNTOS

Intuitivamente un conjunto es una colección (clase, agregado, conglomerado, etc.) de objetos, los cuales pertenecen a (forman parte de, son los elementos de, etc.) el conjunto. En toda teoría axiomática debemos partir de términos que no podemos definir para no correr el riesgo de caer en un círculo vicioso. Tal es el caso de los conceptos de conjunto y pertenencia dentro de la Teoría de Conjuntos. Todas nuestras intuiciones descansan sobre la idea que tengamos de estos conceptos primitivos, sin embargo, para el desarrollo de la teoría no es necesario contar con estas intuiciones.

Temprano en el desarrollo de la teoría de conjuntos se descubrió que esta intuición conducía a contradicciones y que debía descartarse. Esto condujo a una reformulación de la teoría. Existen diversas teorías suficientemente robustas pero que escapan a los objetivos de este curso. Aquí deliberadamente se expondrá una teoría ingenua.

Los axiomas de la teoría ingenua de conjuntos son los siguientes:

Axioma 2.1. *Axioma de Extensión*

Si todo elemento de X es un elemento de Y y todo elemento de Y es un elemento de X, entonces X es igual a Y. Formalmente,

$$\forall XYz((z \in X \leftrightarrow z \in Y) \leftrightarrow X = Y)$$

Dicho de otro modo, si dos conjuntos tienen los mismos elementos, entonces son iguales. Este axioma nos dice que lo que caracteriza a un conjunto son sus elementos.

Axioma 2.2. *Axioma de Comprensión*

Si $P(x)$ es una función proposicional entonces existe el conjunto Y de los elementos que verifican $P(x)$. Formalmente,

$$\exists Y\forall x(x \in Y \leftrightarrow P(x))$$

Esto es lo que se conoce como un *esquema de axiomas*, ya que realmente hay un axioma para cada posible proposición $P(x)$.

A continuación algunos casos importantes:

- Cuando $P(x)$ es la fórmula $falso$, Y es un conjunto que no tiene elementos. Este conjunto es conocido como el conjunto vacío y se le denota $\emptyset$.

- Cuando $P(x)$ es la fórmula $x \notin x$ llegamos a una contradicción. La pregunta es ¿Pertenece Y a Y?. Si la respuesta es afirmativa, entonces Y verifica la propiedad que define a Y (esto es, $Y \notin Y$). Si la respuesta es negativa, entonces, por definición $Y \in Y$. En cualquier caso obtenemos la contradicción:

$$Y \in Y \leftrightarrow Y \notin Y$$

  Esta contradicción se conoce como *paradoja de Russell* y demuestra que este esquema de axiomas (y por lo tanto la teoría ingenua de conjuntos) es inconsistente.
- Cuando $P(x)$ es la fórmula $verdadero$, Y es el conjunto de todo. A este conjunto se le conoce como el conjunto universal o universo o conjunto de todos los conjuntos y se le denotará como U. Se puede demostrar que esto también es inconsistente.

2.1. Inclusión.

Definición 2.3. X es un *subconjunto* de Y o *es parte* de Y (se denota $X \subseteq Y$), si y sólo si todo elemento de X es un elemento de Y. O sea,

$$X \subseteq Y \leftrightarrow \forall x(x \in X \rightarrow x \in Y)$$

Si $X \subseteq Y$ se dice que X está incluido en Y y que Y incluye a X.

Para todo conjunto X se cumple $X \subseteq X$.

Demostración. $\forall x(x \in X \rightarrow x \in X)$ lo cual es trivial. Esta propiedad se llama *reflexividad*. □

Para todo conjunto X, Y se cumple $X \subseteq Y \wedge Y \subseteq X \rightarrow X = Y$.

Demostración. $\forall x((x \in X \rightarrow x \in Y) \wedge (x \in Y \rightarrow x \in X) \rightarrow X = Y)$, por definición de doble implicación esto es lo mismo que decir $\forall x((x \in X \leftrightarrow x \in Y) \rightarrow X = Y)$ y esto no es más que el axioma de extensión. Esta propiedad se denomina *antisimetría*. □

Para todo conjunto X, Y, Z se cumple $X \subseteq Y \wedge Y \subseteq Z \rightarrow X \subseteq Z$

Demostración. $X \subseteq Y \wedge Y \subseteq Z$ equivale a decir $\forall x((x \in X \rightarrow x \in Y) \wedge (x \in Y \rightarrow x \in Z))$. Si esta proposición es cierta, entonces podemos concluir que $\forall x(x \in X \rightarrow x \in Z)$, lo cual es exactamente la definición de $X \subseteq Z$. Esta propiedad se llama *transitividad*. □

Con esta definición, el Axioma 2.1 puede escribirse más abreviadamente como

$$\forall XY(X \subseteq Y \wedge Y \subseteq X \rightarrow X = Y)$$

Definición 2.4. X es un *subconjunto propio* de Y (se denota $X \subset Y$)[1] si $X \subseteq Y \wedge X \neq Y$.

[1]El concepto de subconjunto propio es mucho menos utilizado en la matemática que el de subconjunto. En muchos libros se utiliza el símbolo $\subset$ para indicar la relación de subconjunto que aquí indicamos con el símbolo $\subseteq$.

2.2. Notación.

Definición 2.5. Definición de conjuntos por extensión.

$\{x_1, x_2, \cdots, x_n\}$ denota un conjunto X si y sólo si $\forall y(y \in X \leftrightarrow (y = x_1 \vee y = x_2 \vee \cdots \vee y = x_n))$.

Se podría añadir el requerimiento de que este conjunto debe ser único, pero no es necesario, ya que el Axioma de Extensión lo garantiza.

Ejemplos: $A = \{perro, gato, loro\}$ $B = \{2, 3, 5, 7\}$

Debe tenerse en cuenta que los conceptos primitivos con los que estamos tratando son conjunto y pertenencia. No está definido para un conjunto ningún tipo de orden o multiplicidad en sus elementos. Así $\{1, 2, 3\} = \{3, 2, 1\} = \{2, 2, 1, 1, 3, 3\}$.

Definición 2.6. Definición de conjuntos por comprensión.

$\{x \mid P(x)\}$ denota un conjunto X si y sólo si $\forall z(z \in X \leftrightarrow P(z))$.

Ejemplo: $B = \{x \mid x \in \mathbb{N} \wedge x \text{ es primo} \wedge x \leq 10\}$

3. Operaciones

Definición 3.1. Si C es una colección de conjuntos, la *unión* de C, denotada $\bigcup C$ es el conjunto cuyos elementos son los elementos de los elementos de C. Es decir, z es un elemento de $\bigcup C$ si y sólo si z pertenece a alguno de los conjuntos de la colección C.

$$\bigcup C = \{z \mid \exists X(z \in X \wedge X \in C)\}$$

En particular, la unión de dos conjuntos X y Y, es decir $\bigcup\{X, Y\}$ se denota $X \cup Y$ y es el conjunto que contiene todos los elementos de X y todos los elementos de Y.

$$X \cup Y = \{z \mid z \in X \vee z \in Y\}$$

Ejemplo: Sea $A = \{1, 2\}$ y $B = \{2, 3\}$, entonces $A \cup B = \{1, 2, 3\}$.

Nota: C puede ser un conjunto infinito. Por ejemplo, sea $A_n = \left[\frac{1}{n}, 7\right]$ el intervalo cerrado de números reales entre $\frac{1}{n}$ y 7. Entonces $\bigcup\{A_n\} = (0, 7]$ (para $n = 1, 2, 3, \cdots$).

Definición 3.2. Si C es una colección no vacía de conjuntos, la *intersección* de C, denotada $\bigcap C$ es el conjunto cuyos elementos pertenecen a todos los elementos de C.

$$\bigcap C = \{z \mid \forall X(X \in C \rightarrow z \in X)\}$$

En particular, la intersección de dos conjuntos X y Y, es decir $\bigcap\{X, Y\}$ se denota $X \cap Y$ y es el conjunto cuyos elementos pertenecen a X y a Y.

$$X \cap Y = \{z \mid z \in X \wedge z \in Y\}$$

Ejemplo: Sea $A = \{1, 2\}$ y $B = \{2, 3\}$, entonces $A \cap B = \{2\}$.

Al igual que en el caso de la unión, C puede ser infinito. Para el mismo ejemplo anterior $A_n = \left[\frac{1}{n}, 7\right]$ tenemos que $\bigcap\{A_n\} = [1, 7]$ (para $n = 1, 2, 3, \cdots$).

Definición 3.3. Los conjuntos X y Y son *disjuntos* si $X \cap Y = \emptyset$.

Ejemplo: $A = \{1, 2\}$ y $B = \{gato, perro\}$ son disjuntos.

Definición 3.4. El *complemento* $\overline{X}$ del conjunto X es el conjunto cuyos elementos no pertenecen a X.

$$\overline{X} = \{z \mid z \notin X\}$$

Definición 3.5. La *diferencia* de los conjuntos X y Y se denota $X - Y$ y es el conjunto cuyos elementos pertenecen a X y no pertenecen a Y.

$$X - Y = X \cap \overline{Y} = \{z \mid z \in X \wedge z \notin Y\}$$

Ejemplo: Sea $A = \{1, 2\}$ y $B = \{2, 3\}$, entonces $A - B = \{1\}$.

A continuación algunas propiedades de las operaciones .

Theorem 3.6. *Álgebra de conjuntos.*

Para todo conjunto A,B,C:

1. *Asociatividad*
$$A \cup (B \cup C) = (A \cup B) \cup C,$$
$$A \cap (B \cap C) = (A \cap B) \cap C.$$
2. *Conmutatividad*
$$A \cup B = B \cup A,$$
$$A \cap B = B \cap A.$$
3. *Idempotencia*
$$A \cup A = A,$$
$$A \cap A = A.$$
4. *Absorción*
$$A \cup (A \cap B) = A,$$
$$A \cap (A \cup B) = A.$$
5. *Neutro*
$$A \cup \emptyset = A,$$
$$A \cap U = A.$$
(siendo U un conjunto universal)
6. *Distributividad*
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
7. *Leyes de De Morgan*
$$\overline{A \cup B} = \overline{A} \cap \overline{B},$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$
8. $$A - A = \emptyset$$
9. $$A = (A \cap B) \cup (A - B)$$

Demostración. Ejercicio. □

La relación $A \subseteq B$ se relaciona con las demás operaciones como sigue:

Theorem 3.7. *Para todo conjunto A, B, C, D:*

1. $A \cap B \subseteq A \, y \, A \cap B \subseteq B$
2. $C \subseteq A \wedge C \subseteq B \rightarrow C \subseteq A \cap B$
3. $A \subseteq B \leftrightarrow A \cap B = A$
4. $A \subseteq C \wedge B \subseteq D \rightarrow A \cap B \subseteq C \cap D$
5. $A \subseteq A \cup B \, y \, B \subseteq A \cup B$
6. $A \subseteq B \wedge B \subseteq C \rightarrow A \cup B \subseteq C$
7. $A \subseteq B \leftrightarrow A \cup B = B$
8. $A \subseteq C \wedge B \subseteq D \rightarrow A \cup B \subseteq C \cup D$

Demostración. Ejercicio. □

Ejercicio. Probar que las siguientes proposiciones son equivalentes a $A \subseteq B$:

$$A \cap B = A; \quad A \cup B = B; \quad \overline{B} \subset \overline{A}; \quad B \cup \overline{A} = U; \quad A \cap \overline{B} = \emptyset$$

Definición 3.8. El *conjunto de partes* (también conocido como *conjunto potencia*) del conjunto X se denota $\mathcal{P}(X)$ y es el conjunto cuyos elementos son todos los subconjuntos de X.

$$\mathcal{P}(X) = \{z \mid z \subseteq X\}$$

Nótese que

$$Y \in \mathcal{P}(X) \leftrightarrow Y \subseteq X$$

Ejemplo: Si $A = \{1, 2, 3\}$ entonces $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

A continuación algunas propiedades del conjunto potencia:

Theorem 3.9. *Para todo conjunto A, B:*

1. $\emptyset \in \mathcal{P}(A) \, y \, A \in \mathcal{P}(A)$
2. $\mathcal{P}(\emptyset) = \{\emptyset\}$
3. $A \subseteq B \rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$
4. $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$
5. $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$
6. $\mathcal{P}(A - B) \subseteq (\mathcal{P}(A) - \mathcal{P}(B)) \cup \{\emptyset\}$

Demostración. Ejercicio □

Definición 3.10. Un conjunto P es una *partición* del conjunto A si:

1. $A = \bigcup P$, la unión de los elementos de P es A.
2. $\forall x(x \in P \rightarrow x \neq \emptyset)$, los elementos de P son no vacíos.
3. $\forall xy((x \in P \wedge y \in P \wedge x \neq y) \rightarrow x \cap y = \emptyset)$, los elementos de P son disjuntos dos a dos.

Es decir, A se parte en pedazos.

Ejemplo: Una partición de $\{1, 2, 3, 4, 5\}$ es $\{\{1, 2\}, \{3\}, \{4, 5\}\}$.

4. RELACIONES

Definición 4.1. Dados dos conjuntos a y b llamamos *par ordenado* a, b al siguiente conjunto:

$$(a, b) = \{\{a\}, \{a, b\}\}$$

Nótese que (a, b) es un conjunto.

En el par no ordenado $\{a, b\}$ no podemos distinguir ambos elementos ya que $\{a, b\} = \{b, a\}$. En cambio, los elementos del par ordenado (a, b) sí son distinguibles, es decir, sí sabemos cuál es el primero y cuál es el segundo. $(a, b) = \{\{a\}, \{a, b\}\}$ mientras que $(b, a) = \{\{b\}, \{b, a\}\}$. En consecuencia, $a \neq b \rightarrow (a, b) \neq (b, a)$.

Theorem 4.2. *Si* $(a, b) = (c, d)$ *entonces* $a = c$ *y* $b = d$.

Demostración. Supongamos que $(a, b) = (c, d)$, esto es,

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$$

Si $a = b$ tenemos $\{\{a\}\} = \{\{c\}, \{c, d\}\}$, entonces $\{a\} = \{c\} = \{c, d\}$, o sea, $a = b = c = d$.

Si $a \neq b$ tenemos $\{a\} = \{c\}$ o $\{a\} = \{c, d\}$.

En el primer caso tenemos $a = c$ y como $\{a, b\} \in \{\{c\}, \{c, d\}\}$ y $a \neq b$, $\{a, b\} = \{c, d\}$, por lo tanto $a = c$ y $b = d$.

En el segundo caso tenemos $a = c = d$, por lo tanto $\{a, b\} \in \{\{a\}\}$, o sea $b = a$, lo cual es contradictorio, o sea, que este caso no se puede dar. Por lo tanto si $(a, b) = (c, d)$, entonces $a = c$ y $b = d$. □

Se pueden definir tripletes ordenados, y en general, n-tuplas ordenadas.

$$(a) = \{a\}$$

$$(a, b) = \{\{a\}, \{a, b\}\}$$
$$(a, b, c) = ((a, b), c)$$

$$(a, b, c, d) = ((a, b, c), d)$$
$$(a_1, a_2, \cdots, a_n) = ((a_1, a_2, \cdots, a_{n-1}), a_n)$$

Lema 4.3. *Si* $a \in A$ *y* $b \in A$, $(a, b) \in \mathcal{P}(\mathcal{P}(A))$.

Demostración. Ejercicio. □

Definición 4.4. El *producto cartesiano* de dos conjuntos A y B es el siguiente conjunto:

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Nótese que el producto cartesiano no es conmutativo.

Podemos también introducir productos cartesianos triples, cuádruples, etc., de la siguiente manera:

$$A \times B \times C = \{(a, b, c) \mid a \in A \wedge b \in B \wedge c \in C\}$$
$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}$$

A continuación algunas propiedades de los productos cartesianos:

Theorem 4.5. *Para todo conjunto A, B, C, D:*

1. $A \times \emptyset = \emptyset \times A = \emptyset$
2. $A \neq \emptyset \wedge B \neq \emptyset \rightarrow A \times B \neq \emptyset$
3. $A \subseteq C \wedge B \subseteq D \rightarrow A \times B \subseteq C \times D$
4. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
5. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
6. $A \times (B - C) = (A \times B) - (A \times C)$

Demostración. Ejercicio. □

Definición 4.6. Una *relación* R de un conjunto A en un conjunto B es cualquier subconjunto $R \subseteq A \times B$

Si $A = B$ se dice que R es una relación en A.

Con frecuencia, la expresión $(a, b) \in R$ se abrevia aRb.

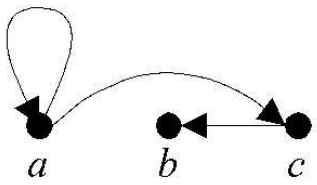
Definición 4.7. *Dominio y recorrido* de una relación son los conjuntos $Dom(R) = \{a \mid \exists b((a, b) \in R)\}$ y $Rec(R) = \{b \mid \exists a((a, b) \in R)\}$

Formas de representar las relaciones:

- Diagrama de flechas entre dos conjuntos
- Como matrices de elementos $\{0, 1\}$. Ejemplo: $\{(a, x), (a, z), (b, y), (b, w), (c, x), (c, w)\}$ se representa como

	x	y	w	z
a	1	0	0	1
b	0	1	1	0
c	1	0	1	0

- Como un grafo cuando la relación es en un conjunto A.
  Ejemplo: $R = \{(a, a), (a, c), (c, b)\}$con $A = \{a, b, c\}$ se representa como



Definición 4.8. Si R es una relación de A en B y S es una relación de B en C, entonces la *composición de R y S* es la relación $S \circ R$ de A en C definida como

$$S \circ R = \{(a, c) \mid \exists b((a, b) \in R \wedge (b, c) \in S)\}$$

Si se utiliza representación matricial para representar las relaciones R y S, entonces la representación matricial de $S \circ R$ es la multiplicación de las matrices de R y S (asumiendo que cualquier suma cuyo resultado sea distinto de 0 es 1, en particular $1 + 1 = 1$).

Obsérvese la inversión de R y S en la notación de la composición.

A continuación algunas propiedades de la composición de relaciones:

Theorem 4.9. *Si R, S y T son relaciones, entonces:*

1. $(T \circ S) \circ R = T \circ (S \circ R)$

2. $(S \cup T) \circ R = (S \circ R) \cup (T \circ R)$
3. $T \circ (S \cup R) = (T \circ S) \cup (T \circ R)$
4. $(S \cap T) \circ R \subseteq (S \circ R) \cap (T \circ R)$
5. $T \circ (S \cap R) \subseteq (T \circ S) \cap (T \circ R)$
6. $R \subseteq S \rightarrow T \circ R \subseteq T \circ S$
7. $R \subseteq S \rightarrow R \circ T \subseteq S \circ T$

Demostración. Ejercicio. □

Definición 4.10. La *relación inversa* de R es la relación $R^{-1} = \{(b, a) \mid (a, b) \in R\}$.

Si se utiliza representación matricial para representar la relación R, entonces la representación de R^{-1} es la traspuesta de R (las filas de R pasan a ser las columnas de R^{-1}). Si se utiliza la notación de grafos, R^{-1}sería igual que R pero cambiando el sentido de las flechas.

A continuación algunas propiedades de las relaciones inversas:

Theorem 4.11. *Si R y S son relaciones, entonces:*

1. $\left(R^{-1}\right)^{-1} = R$
2. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Demostración. Ejercicio. □

Existen algunas relaciones que tienen un rol fundamental en la matemática y por lo tanto se estudiarán con mayor detenimiento en las secciones siguientes.

5. Relaciones de Equivalencia

Definición 5.1. Sea R una relación en A

1. R es *refleja* si $\forall a(a \in A \rightarrow (a, a) \in R)$
2. R es *simétrica* si $\forall ab((a, b) \in R \rightarrow (b, a) \in R)$
3. R es *transitiva* si $\forall abc(((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R)$
4. R es de *equivalencia* si y sólo si R es refleja, simétrica y transitiva.

Ejemplo: Igualdad, paralelismo de rectas, $(a, b)R(c, d) \leftrightarrow ad = bc$

Si se representa una relación refleja utilizando notación matricial, entonces la diagonal de la matriz tiene sólo unos.

Si se representa una relación refleja utilizando notación de grafo, entonces todos los vértices tienen un arco que sale y llega al mismo vértice.

Si se representa una relación simétrica utilizando notación matricial, entonces la matriz es simétrica con respecto a la diagonal.

Si se representa una relación simétrica utilizando notación de grafo, entonces cada vez que hay un arco de un vértice a a un vértice b también hay un arco del vértice b al vértice a. Puede haber arcos que salen y llegan al mismo vértice, en cuyo caso no se repite el arco.

Definición 5.2. Sea R una relación de equivalencia en A y $x \in A$. La clase de equivalencia de x se define como $C_x = \{y \mid (x, y) \in R\}$.

Theorem 5.3. *Sea R una relación de equivalencia en A y sean $x, y \in A$.*

1. $x \in C_x$
2. $(x, y) \in R \leftrightarrow C_x = C_y$

3. $C_x \cap C_y \neq \emptyset \rightarrow C_x = C_y$
4. $x \in C_y \rightarrow C_x = C_y$
5. $x, y \in C_z \rightarrow C_x = C_y$

Demostración. Ejercicio. □

Toda relación de equivalencia sobre un conjunto da origen a una única partición de ese conjunto y toda partición de un conjunto da origen a una única relación de equivalencia.

Theorem 5.4. *Si R es de equivalencia en A entonces el conjunto de las clases C_x constituye una partición de A.*

Demostración. Por 1, las clases son no vacías y todo elemento pertenece a alguna clase. Por 3, las clases son disjuntas.

□

Definición 5.5. La partición generada por las clases de equivalencia de una relación de equivalencia R se denomina *conjunto cociente*. El conjunto cociente de una relación de equivalencia R en A se denota A/R.

Por ejemplo, el conjunto cociente asociado a la relación de equivalencia de paralelismo entre rectas puede interpretarse como el conjunto de las direcciones.

Theorem 5.6. *Si P es una partición de A entonces la relación $R = \{(x, y) \mid \exists z(z \in P \wedge \{x, y\} \subseteq z)\}$ es una relación de equivalencia en A.*

Demostración. Sea P una partición de A.

Para $x \in A$, como $A = \bigcup P$, existe una $z \in P$ tal que $x \in z$, o sea $\{x\} \subseteq z$. Por lo tanto $(x, x) \in R$ y R es refleja.

Si para algún $z \in P$, $\{x, y\} \subseteq z$, entonces $\{y, x\} \subseteq z$. Por lo tanto R es simétrica.

Si existen $u_1, u_2 \in P$ tales que $\{x, y\} \subseteq u_1$ y $\{y, z\} \subseteq u_2$, entonces $u_1 \cap u_2 \neq \emptyset$ y por lo tanto $u_1 = u_2$. Por lo tanto $\{x, z\} \subseteq u_1$, o sea, R es transitiva. □

6. Relaciones de Orden

Definición 6.1. Sea R una relación en A y $x, y \in A$:

1. R es *antisimétrica* si $xRy \wedge yRx \rightarrow x = y$.
2. R es *total* si $xRy \vee yRx$.
3. R es un *orden* si y sólo si R es refleja, antisimétrica y transitiva.
4. R es un *orden total* si R es de orden y total.

Habitualmente los órdenes se designan con los símbolos $\leq$ o $\preceq$. Con frecuencia, $a \leq b$ se representa como $b \geq a$. Entonces $\geq$ sería la relación inversa de $\leq$.

Ejemplos:

- Los números reales con su orden usual constituyen un conjunto totalmente ordenado.
- Los números naturales se pueden ordenar parcialmente de la siguiente manera: dados dos números naturales m y n definimos $m \preceq n$ si y sólo si m divide a n.

- La relación de inclusión puede verse como un orden parcial del conjunto de todos los conjuntos[2] .

Definición 6.2. Sea $\leq$ un orden de A. Supongamos que $X \subseteq A$, $a \in A$ y $x \in X$:

1. a es un *elemento maximal* de X si $a \in X \wedge (a \leq x \rightarrow x = a)$. Si existe un único maximal, éste recibe el nombre de *máximo* o *mayor elemento*.
2. a es una *cota superior* de X si $\forall x(x \leq a)$.
3. a es el *supremo* de X si a es la menor cota superior de X. Si a es el supremo de X y $a \in X$ entonces a es el máximo de X

Nótese que puede haber varios elementos maximales, pero no más de un supremo. Si existe un máximo, éste es el único elemento maximal.

Los conceptos de *elemento minimal*, *cota inferior*, *ínfimo* y *menor elemento* se definen análogamente:

1. a es un *elemento mínimal* de X si $a \in X \wedge (x \leq a \rightarrow x = a)$. Si existe un único minimal, éste recibe el nombre de *mínimo* o menor *elemento*.
2. a es una *cota inferior* de X si $\forall x(a \leq x)$.
3. a es el *ínfimo* de X si a es la mayor cota inferior de X. Si a es el ínfimo de X y $a \in X$, a es el mínimo de X.

Ejemplos:

- Considérese el conjunto de los números reales mayores que 0 y menores que 1. El ínfimo es 0, el supremo es 1. No hay elementos minimales o maximales.
- Sea $A = \{1, 2, 3, 6, 9, 14\}$, $X = \{2, 3, 6, 9, 14\}$ y $\leq = \{(a, b) \mid a \text{ divide a } b\}$ es la relación de orden en A. En este caso 2 y 3 son elementos minimales de X. 1 es el ínfimo de X. 6, 9 y 14 son elementos maximales de X y no hay supremo.

Definición 6.3. Sea $\leq$ una relación de orden en A.

$\leq$ es un *buen orden* si todo subconjunto no vacío de A tiene un elemento mínimo.

Un conjunto X con un buen orden $\leq$ (el par ordenado $(X, \leq)$) se denomina *conjunto bien ordenado*.

Theorem 6.4. *Un buen orden siempre es un orden total.*

Demostración. Supongamos que x y y son elementos de un conjunto bien ordenado, entonces $\{x, y\}$ es un conjunto no vacío de ese conjunto bien ordenado y por lo tanto tiene un mínimo elemento, el cual es x o y según sea que $x \leq y$ o $y \leq x$. □

Ejemplo: números naturales.

En un conjunto bien ordenado todo elemento, a menos que sea el máximo, tiene un único sucesor: el mínimo elemento mayor que él. Sin embargo, no todo elemento tiene que tener un predecesor.

Ejemplo: Considérense dos copias de los números naturales ordenadas de manera tal que todos los elementos de la primera copia son menores que los de la segunda copia. Dentro de cada copia se utiliza la definición habitual de orden. Nótese que mientras que todo elemento tiene un sucesor, hay dos elementos que no tienen predecesor: el cero de la primera copia y el cero de la segunda copia. La lista sería algo como $0, 1, 2, 3, \cdots, 0', 1', 2', 3', \cdots$.

Definición 6.5. Sea R una relación en A y $x, y \in A$:

[2]Recuérdese que este conjunto de todos los conjuntos es una inconsistencia de la teoría ingenua de conjuntos. Una manera más correcta de definir este orden sería la relación de inclusión en un conjunto de conjuntos dado (e.g. el conjunto de partes de un conjunto).

1. R es *asimétrica* si $\forall xy((x \in A \wedge y \in A \wedge xRy) \rightarrow \neg yRx$.
2. R es un *orden estricto* si R es de asimétrica y transitiva.

Habitualmente los órdenes estrictos se designan con los símbolos $<$ o $\prec$. Con frecuencia, $a < b$ se representa como $b > a$. Entonces $>$ sería la relación inversa de $<$.

7. FUNCIONES

Definición 7.1. $F : X \longrightarrow Y$ es una *función* si y sólo si:

1. F es una relación de X en Y.
2. $Dom(F) = X$, es decir, todo elemento del conjunto X tiene una imagen.
3. $(x, y) \in F \wedge (x, z) \in F \rightarrow y = z$, es decir, la imagen de cada elemento $x \in X$ es única.

Las funciones son las relaciones más importantes y se encuentran en casi todos los temas matemáticos.

Con frecuencia se escribe $F(x) = y$ cuando F es una función y $(x, y) \in F$.

7.1. Tipos de Funciones.

Definición 7.2. Una función $F : X \longrightarrow Y$ es *inyectiva* o *uno a uno* si se cumple $\forall xy(F(x) = F(y) \rightarrow x = y)$. Es decir, a cada elemento de X corresponde una imagen distinta en Y.

Definición 7.3. Una función $F : X \longrightarrow Y$ es *sobreyectiva,* o simplemente *sobre,* si se cumple $\forall y(y \in Y \rightarrow \exists x(x \in X \wedge y = F(x))$. Es decir, todo elemento de Y es imagen de algún elemento de X.

Definición 7.4. Una función $F : X \longrightarrow Y$ es *biyectiva* si es inyectiva y sobreyectiva.

El concepto de *función biyectiva* con frecuencia recibe el nombre de *biyección* y *correspondencia biunívoca*.

Si una función $F : X \longrightarrow Y$ es biyectiva entonces existe la función inversa $F^{-1} : Y \longrightarrow X$ definida como $F^{-1} = \{(y, x) \mid (x, y) \in F\}$.

7.2. Composición de funciones.

Definición 7.5. Supóngase que g es una función de X en Y y que f es una función de Y en Z. Dado un $x \in X$, podemos aplicarle g para determinar un único elemento $y = g(x) \in Y$. Luego podemos aplicar f para determinar un único elemento $z = f(y) = f(g(x)) \in Z$. La función resultante de X en Z es la *composición de f con g* y se denota $f \circ g$.

Ejemplo: Sea

$$g = \{(1, a), (2, a), (3, c)\}$$

una función de $X = \{1, 2, 3\}$ en $Y = \{a, b, c\}$, y

$$f = \{(a, y), (b, x), (c, z)\}$$

una función de $Y = \{a, b, c\}$ en $Z = \{x, y, z\}$.

La composición de f con g es la función de X en Z: $f \circ g = \{(1, y), (2, y), (3, z)\}$.

Utilizando notación matricial para representar las funciones se puede obtener $f \circ g$ mediante la multiplicación de la matriz asociada a g y la matriz asociada a f.

8. Números Naturales

Los números naturales sirven para contar y enumerar los conjuntos finitos. A continuación se definirán formalmente los números naturales.

Definición 8.1. El *sucesor* de un conjunto x es el conjunto

$$S(x) = x \cup \{x\}.$$

Nótese que los elementos de $S(x)$ son x y los elementos de x, por lo tanto $y \in S(x)$ si y sólo si $y \in x$ o $y = x$.

Definición 8.2. Un conjunto C es *inductivo* o *de sucesores* si:

1. $\emptyset \in C$
2. $x \in C \to S(x) \in C$

Definición 8.3. El conjunto de los *números naturales* se define como la intersección de todos los conjuntos inductivos y es, por lo tanto, el conjunto inductivo más "pequeño" de todos. Nótese que el único elemento de los naturales que no es sucesor de ningún otro elemento es el conjunto vacío (el 0). Denotaremos como $\mathbb{N}$ al conjunto de los números naturales.

Los números naturales se denotarán de la siguiente manera:

$$\begin{aligned}
0 &= \emptyset \\
1 &= S(0) = \{\emptyset\} \\
2 &= S(1) = \{\emptyset, \{\emptyset\}\} = \{0, 1\} \\
3 &= S(2) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\} \\
&\vdots
\end{aligned}$$

La definición anterior introduce los números naturales en forma bastante sencilla. Debemos destacar algunas características de ésta. En primer lugar 0 es un número natural. En segundo lugar, si n es un número natural, entonces su sucesor también lo es. En tercer lugar todo número natural corresponde a una de esas dos posibilidades, o es 0 o es el sucesor de algún otro número natural.

Una segunda observación intuitiva es que el número natural n contiene n elementos. Por ejemplo, 0 no contiene ningún elemento, 1 contiene un elemento, 2 contiene dos, etc.

En general, $S(n) = \{0, 1, 2, \cdots, n\}$, todo número natural está formado por los naturales que lo preceden, salvo el 0, que no contiene ningún elemento.

Nótese que $0 \in 1 \in 2 \in 3 \in \cdots$ y también $0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq \cdots$. Esta observación nos indica que la inclusión entre naturales define un orden total. De hecho, los naturales se definen de esta manera para que la relación de inclusión sea un buen orden.

8.1. Axiomas de Peano. Peano propuso los siguientes axiomas para definir los números naturales:

1. Existe el número natural 0.
2. Todo número natural a tiene un sucesor, denotado por $S(a)$
3. No existe ningún número natural cuyo sucesor es 0.
4. Si $C \subseteq \mathbb{N}$, si se cumple $0 \in C \wedge (n \in C \to S(n) \in C)$, entonces $C = \mathbb{N}$.
5. Números naturales distintos tienen sucesores distintos: $a \neq b \to S(a) \neq S(b)$, o lo que es lo mismo, $S(a) = S(b) \to a = b$.

En nuestro caso, los números naturales fueron construidos a partir de conjuntos. En esta sección se demostrará que los números construidos cumplen con los axiomas de Peano.

1. $\emptyset = 0 \in \mathbb{N}$, ya que $\mathbb{N}$ es inductivo.
2. Si $a \in \mathbb{N}$ entonces $S(a) \in \mathbb{N}$, ya que $\mathbb{N}$ es inductivo.
3. Por definición, $n \in S(n)$, entonces es claro que $S(n)$ no es 0, ya que 0 no contiene ningún elemento.
4. La propiedad minimal de $\mathbb{N}$ hace que si C es inductivo y es un subconjunto de $\mathbb{N}$ entonces $C = \mathbb{N}$. Este axioma se conoce como *principio de inducción*.
5. La demostración del Axioma 5 no es trivial. Para demostrarlo hay que demostrar primero los siguientes teoremas:

   Theorem 8.4. *Ningún número natural es subconjunto de ninguno de sus elementos.* $\forall n \in \mathbb{N}(m \in n \rightarrow n \nsubseteq m)$ *o, equivalentemente* $\forall n \in \mathbb{N}(n \subseteq m \rightarrow m \notin n)$

   Demostración. Para demostrar esto utilizaremos el principio de inducción. Sea X el conjunto de aquellos números naturales n que no son subconjunto de ninguno de sus elementos. Puesto que 0 no es subconjunto de ninguno de sus elementos se cumple que $0 \in X$. Supongamos que $n \in X$, entonces hay que demostrar que $S(n) \in X$. Para que esto sea cierto $S(n)$ no puede ser subconjunto ni de n ni de ningún elemento de n, ya que $S(n) = n \cup \{n\}$. Se sabe que $n \subseteq n$, entonces, por hipótesis $n \notin n$ y por lo tanto $S(n) \nsubseteq n$. Falta demostrar que $S(n)$ no es subconjunto de ningún elemento de n. Supongamos que $S(n) \subseteq x$, entonces $n \subseteq x$ y, por hipótesis, $x \notin n$, entonces $S(n)$ no puede ser subconjunto de ningún elemento de n. Se concluye que $S(n) \in X$ y por lo tanto $X = \mathbb{N}$.

   □

   Theorem 8.5. *Todo elemento de un número natural es subconjunto de dicho número natural.* $\forall n \in \mathbb{N}(m \in n \rightarrow m \subseteq n)$

   Demostración. Esta demostración también es inductiva. Sea X el conjunto de todos lo naturales que cumplen la propiedad indicada. El requerimiento se cumple trivialmente para 0. Supongamos que $n \in X$. Si $x \in S(n)$ entonces, por definición, $x \in n$ o $x = n$. En el primer caso, por hipótesis $x \subseteq n$ y por lo tanto $x \subseteq S(n)$. En el segundo caso, obviamente, $x \subseteq S(n)$. Se concluye que todos los elementos de $S(n)$ son subconjuntos de $S(n)$ y, por lo tanto, $S(n) \in X$ y $X = \mathbb{N}$. □

   Ahora estamos listos para demostrar el Axioma 5. Supóngase que a y b son números naturales y que $S(a) = S(b)$. Puesto que $a \in S(a)$, $a \in S(b)$ y por lo tanto $a \in b$ o $a = b$. El mismo razonamiento aplica para llegar a la conclusión de que $b \in a$ o $b = a$. Si $a \neq b$ entonces $a \in b$ y $b \in a$. Por el Teorema 8.4 concluimos que $b \nsubseteq a$ y por el Teorema 8.5 concluimos que $b \subseteq a$, lo cual es una contradicción; y que $a \nsubseteq b$ y $a \subseteq b$, lo cual también es contradictorio. Entonces es imposible que $a \neq b$ y por lo tanto $S(a) = S(b) \rightarrow a = b$.

El principio de inducción (Axioma 4) puede ser enunciado en términos de la proposición lógica que define al conjunto C por comprensión.

Theorem 8.6. *Sea $\varphi(x)$ una función proposicional. Supongamos que*

1. $\varphi(0)$ se verifica
2. Para todo $n \in \mathbb{N}$, si $\varphi(n)$ se verifica, entonces $\varphi(S(n))$ también se verifica

Entonces $\varphi(n)$ se verifica para todo $n \in \mathbb{N}$.

Demostración. Sea X el conjunto de los números naturales para los que se verifica $\varphi(x)$, $X = \{x \in \mathbb{N} \mid \varphi(x)\}$. $0 \in X$ ya que $\varphi(0)$ se verifica. Supongamos que $n \in X$, entonces $\varphi(n)$ se verifica y por hipótesis $\varphi(S(n))$ se verifica y $S(n) \in X$. Por lo tanto X es inductivo. Como $X \subseteq \mathbb{N}$, entonces $X = \mathbb{N}$. □

8.2. Orden en los números naturales.

Definición 8.7. La relación $\leq$ se define en $\mathbb{N}$ por:

$$m \leq n \leftrightarrow m \in n \vee m = n$$

En este caso diremos m es menor o igual a n.

Utilizaremos el símbolo $<$ para denotar la relación

$$m < n \leftrightarrow m \leq n \wedge m \neq n \leftrightarrow m \in n$$

En este caso diremos m es menor que n.

Lema 8.8. *Para todo número natural m, n, p se cumple que $m \in n \wedge n \in p \rightarrow m \in p$.*

Demostración. Supongamos que $n \in p$, entonces por el Teoremas 8.5 $n \subseteq p$. Si adicionalmente $m \in n$, entonces $m \in p$. Por lo tanto $m \in n \wedge n \in p \rightarrow m \in p$. □

Lema 8.9. *Para todo número natural m, n se cumple que $m \in n \rightarrow S(m) \in S(n)$.*

Demostración. Por inducción en n.

1. Para $n = 0$ la propiedad es verdadera trivialmente, ya que $m \in 0$ siempre es falsa.
2. Asumiendo $m \in n \rightarrow S(m) \in S(n)$ se debe verificar que $m \in S(n) \rightarrow S(m) \in S(S(n))$. Nótese que $S(m) \in S(S(n))$ si y sólo si $S(m) = S(n)$ o $S(m) \in S(n)$. Asumamos que $m \in S(n)$, entonces $m = n$ o $m \in n$. Si $m = n$ tenemos $S(m) = S(n)$; si $m \in n$, por hipótesis inductiva tenemos $S(m) \in S(n)$.

Por lo tanto $m \in n \rightarrow S(m) \in S(n)$ se verifica para todo $m, n \in \mathbb{N}$.

□

Theorem 8.10. *$\leq$ es un orden total sobre $\mathbb{N}$.*

Demostración. Se debe demostrar que $\leq$ es refleja, antisimétrica, transitiva y total. Supóngase que m, n y k son números naturales.

1. Reflexividad. $n \leq n$ trivialmente para todo $n \in \mathbb{N}$ ya que $n = n$.
2. Antisimetría: $m \leq n \wedge n \leq m \rightarrow m = n$. Supongamos que $m \leq n \wedge n \leq m$ se cumple, pero $m \neq n$. Entonces se cumple $m \in n \wedge n \in m$. Por el Teorema 8.5 entonces $m \subseteq n$ y $n \subseteq m$, lo cual implica $m = n$ (ver Teorema 2.1).
3. Transitividad: $k \leq m \wedge m \leq n \rightarrow k \leq n$. Si $k = m$ o $k = n$ la propiedad se cumple trivialmente. Supongamos que $k \in m$ y $m \in n$, entonces, por el Lema 8.8, $k \in n$ y por lo tanto $k \leq n$.

□

1. Totalidad: Se debe cumplir $m \leq n \vee n \leq m$. Por definición, esto equivale a decir $m \in n \vee m = n \vee n \in m$. Se utilizará inducción en n para demostrar que la propiedad se cumple:
   a) Para $n = 0$ se debe cumplir $m = 0 \vee 0 \in m$. Para demostrar esto se utilizará inducción en m.
      1) Para $m = 0$ la condición se verifica trivialmente.
      2) Se debe verificar ahora que $m = 0 \vee 0 \in m \rightarrow S(m) = 0 \vee 0 \in S(m)$. $S(m) = 0$ es imposible, así que hay que demostrar que $m = 0 \vee 0 \in m \rightarrow 0 \in S(m)$. Si $m = 0$ entonces $S(m) = 0 \cup \{0\} = \{0\}$, entonces $0 \in S(m)$ y la propiedad se verifica. Por hipótesis, $0 \in m$ y, por definición, se sabe que $m \in S(m)$, entonces por el Lema 8.8, $0 \in S(m)$ y por lo tanto se verifica la propiedad.

Por lo tanto la propiedad se verifica para $n = 0$.

b) Ahora se debe verificar que $m \in n \vee m = n \vee n \in m \rightarrow m \in S(n) \vee m = S(n) \vee S(n) \in m$. Supóngase que $m \in n$; por definición $n \in S(n)$; entonces por el Lema 8.8, $m \in S(n)$ y se verifica la propiedad.
Supóngase que $m = n$; por definición $n \in S(n)$ y por lo tanto $m \in S(n)$ y se verifica la propiedad.
Supóngase que $n \in m$, entonces $m \neq 0$ y podemos decir que $m = S(k)$ y $n \in S(k)$. Entonces tenemos que $n = k$ o $n \in k$. Si $n = k$, entonces $S(n) = S(k) = m$, lo cual verifica la propiedad. Si $n \in k$ entonces, por el Lema 8.9, $S(n) \in S(k) = m$, lo cual verifica la propiedad.

Por lo tanto para todo $m, n \in \mathbb{N}$ se cumple que $m \leq n \vee n \leq m$.

Corolario 8.11. *Tricotomía. Para todo $m, n \in \mathbb{N}$ se cumple una y sólo una de las siguientes propiedades: $m < n$, $m = n$, $n < m$.*

Demostración. Por el teorema 8.10 se sabe que $m \in n \vee m = n \vee n \in m$. Falta sólo verificar que sólo una de ellas se cumple.

Supongamos $m < n$, o lo que es lo mismo, $m \in n$, entonces, por el Teorema 8.4, $n \notin m$. Si $n \in m$ o $n = m$ entonces $n \subseteq m$ (Teorema 8.5), con lo cual llegamos a una contradicción.

El mismo razonamiento aplica si $n < m$.

Si $m = n$ esto equivale a $m \subseteq n \wedge n \subseteq m$. Si $m < n$ entonces $n \notin m$ y llegamos a una contradicción. Lo mismo aplica si $n < m$. □

Theorem 8.12. $\leq$ *es un buen orden*

Demostración. Sea X un subconjunto de $\mathbb{N}$. Debemos demostrar que X tiene un mínimo o que $X = \emptyset$. Sea $\varphi(n)$ la proposición "ningún elemento de X es menor que n" (más formalmente, $\forall k(k < n \rightarrow k \notin X)$). Si X tiene un mínimo entonces no hay problema ya que ningún elemento de X es menor que su mínimo. Supongamos que X no tiene mínimo y apliquemos inducción en n.

1. $\varphi(0)$ es verdadera, ya que ningún elemento puede ser menor que 0.
2. Supóngase que $\varphi(n)$ es verdadera. Si $\varphi(S(n))$ fuera falsa, entonces X tendría un elemento menor que $S(n)$, pero no podría ser menor que n ya que $\varphi(n)$ se verifica y n sería el mínimo, lo cual sería una contradicción. Entonces $\varphi(S(n))$ se verifica y por lo tanto $\varphi(n)$ se verifica para todo n.

Por lo tanto, para todo n, ningún elemento de X es menor que n. Esto sólo puede ser cierto si X no tiene elementos, ya que, por definición, todo número natural es menor que su sucesor.

□

Nótese que en algunos casos se utiliza el buen orden de los naturales como un axioma denominado *Principio de buena ordenación de los números naturales* o simplemente, *principio de buena ordenación*. El principio de inducción se puede demostrar a partir del principio de buena ordenación. Esto significa que ambos principios son equivalentes. Queda como ejercicio demostrar el principio de inducción a partir del principio de buena ordenación.

8.3. Aritmética en los números naturales. Una operación binaria (también llamada operador binario) en un conjunto A es una función $Q : A \times A \longrightarrow A$. Usualmente el elemento $((a, b), c)$ de Q se suele escribir $a\,Q\,b = c$ y en algunos casos $Q(a, b) = c$.

8.3.1. Adición. La adición es una operación binaria identificada con el símbolo $+$ ($+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$) definida por las siguientes propiedades:

$$a + 0 = a$$

$$a + S(b) = S(a + b)$$

El resultado de esta operación se llama *suma*.

La adición tiene las siguientes propiedades:

- Asociativa: $(a + b) + c = a + (b + c)$
- Conmutativa: $a + b = b + a$

Las demostraciones se dejan como ejercicio.

8.3.2. Multiplicación. La multiplicación es una operación binaria identificada con el símbolo $\cdot$ ($\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$). definida por las siguientes propiedades:

$$a \cdot 0 = 0$$

$$a \cdot S(b) = a \cdot b + a$$

Con mucha frecuencia, se omite el símbolo de multiplicación, y escribimos ab en lugar de $a \cdot b$.

El resultado de esta operación se llama *producto*.

A veces se utiliza para la multiplicación el símbolo $\times$, pero aquí no lo usaremos para evitar confusión con el producto cartesiano.

La multiplicación tiene las siguientes propiedades:

- Asociativa: $(ab)c = a(bc)$
- Conmutativa: $ab = ba$
- Distributiva: $a(b + c) = ab + ac$

Las demostraciones se dejan como ejercicio.

El orden en los naturales es compatible con las operaciones aritméticas. Para todo natural a, b, c se cumple:

$$a \leq b \rightarrow a + c \leq b + c$$
$$a \leq b \rightarrow ac \leq bc$$

9. CARDINALIDAD

Definición 9.1. Dos conjuntos A y B tienen la misma *cardinalidad* si y sólo si existe una función biyectiva entre A y B. En tal caso escribimos $A \sim B$. En ocasiones $A \sim B$ se lee A es *equinumeroso* con B, A es *coordinable* con B o A es *equipolente* a B.

Podemos ver la cardinalidad como una relación de equivalencia[3] ya que se puede demostrar que $A \sim A$, $A \sim B \rightarrow B \sim A$ y $A \sim B \wedge B \sim C \rightarrow A \sim C$.

Definición 9.2. Un conjunto es *finito* si tiene la misma cardinalidad que algún número natural.

Definición 9.3. Un conjunto *infinito* es aquel que no es finito.

Un conjunto I es infinito si y sólo si tiene algún subconjunto propio S tal que $I \sim S$.

[3]Esta relación sería en el conjunto de todos los conjuntos (U). Recuérdese que es imposible que exista el conjunto universal y por lo tanto esta definición de cardinalidad es inadecuada si se estudia una teoría más robusta.

Definición 9.4. Un *número cardinal* o simplemente *cardinal* es una clase de equivalencia (un elemento del conjunto cociente) de la relación de *cardinalidad*. El cardinal del conjunto A se denota $|A|$.

Cada número natural corresponde a un número cardinal finito diferente.

$\mathbb{N}$ es el conjunto infinito con menor cardinalidad.

Definición 9.5. Existe un orden $\leq$ en los cardinales. $|A| \leq |B|$ si existe una función inyectiva de A en B. Así, para todo par de conjuntos A, B se cumple $|A| \leq |B| \vee |B| \leq |A|$. Como es usual, se utilizará $|A| < |B|$ para indicar $|A| \leq |B| \wedge |A| \neq |B|$. Nota: se debe demostrar que $\leq$ es un orden total.

Para representar los cardinales finitos se utilizarán los mismos símbolos utilizados para representar los números naturales $(0, 1, 2, \cdots)$. Por el contexto se sabrá si se trata de un número natural o un cardinal.

Para representar los cardinales infinitos se utilizará una notación con la letra hebrea $\aleph$ (aleph) . El menor cardinal infinito es $\aleph_0$ y es igual a $|\mathbb{N}|$. $\aleph_1$ denota el siguiente cardinal infinito. No existe ningún conjunto A tal que $\aleph_0 < |A| < \aleph_1$. Evidentemente, si n es un cardinal finito entonces $n < \aleph_0$.

La cardinalidad del conjunto de los números reales se suele denotar con la letra c y se denomina *continuo*. $c > \aleph_0$.

Definición 9.6. Un conjunto A es *contable* o *enumerable* si $|A| \leq \aleph_0$. Si $|A| = \aleph_0$ entonces A es un conjunto *contablemente infinito*. Todos los elementos de un conjunto enumerable se pueden enumerar uno tras otro en una lista (suponiendo que haya suficiente papel, tinta, energía y tiempo en el universo para elaborar dicha lista).

Teorema de Cantor. Para todo conjunto A se cumple que $|A| < |\mathcal{P}(A)|$.

Demostración. Se debe demostrar que toda función inyectiva $f : A \longrightarrow \mathcal{P}(A)$ no puede ser sobreyectiva. Para esto basta mostrar un subconjunto de A (un elemento de $\mathcal{P}(A)$) que no esté en el recorrido de f. Un subconjunto que cumple con esa condición es $B = \{x \in A \mid x \notin f(x)\}$.

Supóngase que B está en el recorrido de f. Entonces, para algún $a \in A$ tendremos $f(a) = B$. Ahora hay que determinar si $a \in B$. Si $a \in B$ entonces $a \in f(a)$, pero eso implica, por definición que $a \notin f(a)$. Por otro lado, si $a \notin B$ entonces $a \notin f(a)$ y por lo tanto $a \in B$. En cualquier caso obtenemos la contradicción $a \in B \leftrightarrow a \notin B$. □

10. Números Enteros

Para definir nuevos conjuntos de números se utiliza un método denominado *genético*. Es decir, cada nuevo conjunto de números se define en términos de un conjunto previo. Existen tres ideas fundamentales por las cuales se definen nuevos conjuntos de números:

1. Ampliar el conjunto.
2. Hacer cosas que no se podían hacer con el conjunto previo.
3. Conservar las propiedades (operaciones y orden) existentes en el conjunto previo para los números equivalentes en el nuevo conjunto.

La motivación principal para definir los números enteros es permitir la operación de resta entre cualquier par de números, cosa que no es posible en los números naturales.

Definición 10.1. Sea $\mathcal{Z}$ la relación de equivalencia en $\mathbb{N} \times \mathbb{N}$ tal que $(m, n)\mathcal{Z}(p, q)$ si $m + q = n + p$. Formalmente,

$$\mathcal{Z} = \{((m, n), (p, q)) \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \mid m + q = n + p\}$$

El conjunto de los números enteros es el conjunto cociente de la relación $\mathcal{Z}$ y se denota con el símbolo $\mathbb{Z}$. Formalmente,

$$\mathbb{Z} = \mathbb{N}\times\mathbb{N}/\mathcal{Z}$$

Cada clase de equivalencia de la relación $\mathcal{Z}$ es un número entero.

Bajo la relación de equivalencia $\mathcal{Z}$ tenemos que $(1, 0)$, $(2, 1)$ y $(8, 7)$ pertenecen a la misma clase de equivalencia. Igualmente, $(1, 4)$, $(3, 6)$ y $(7, 10)$ son equivalentes. Para representar a un número entero normalmente se escoge como representante de la clase al elemento que tenga el natural 0 como alguna de sus componentes. Entonces, para el primer ejemplo, el representante preferido es $(1, 0)$ y para el segundo sería $(0, 3)$. Usualmente cuando la segunda componente es cero, el entero se representa con el número natural de la primera componente, así en el primer ejemplo el número entero se representaría con el símbolo 1 y en general, cuando el representante preferido es $(a, 0)$ (con $a \in \mathbb{N}$) el entero se representará como a. Cuando la primera componente es cero, el entero se representa con el número natural de la segunda componente precedido por el símbolo $-$, así en el segundo ejemplo el número entero se representaría con el símbolo -3 y en general, cuando el representante preferido tiene la forma $(0, a)$ el entero se representará como $-a$. Todo entero a tiene un opuesto $-a$. $-(-a) = a$. En el caso particular en que el entero es la clase del par $(0, 0)$ la representación utilizada es 0. En todo caso, por el contexto se sabrá si un símbolo representa un natural o un entero.

En lo que resta de esta sección utilizaremos la notación $[a, b]$ para representar al número entero $C_{(a,b)}$, es decir, a la clase de equivalencia a la que pertenece el par de números naturales (a, b).

10.1. Orden en los números enteros. Para los números enteros se define la relación de orden $\leq$ como:

$$[m, n] \leq [p, q] \leftrightarrow m + q \leq n + p$$

Esta es una relación de orden total, pero no es un buen orden. Las demostraciones se dejan como ejercicio.

El orden en los enteros es compatible con las operaciones aritméticas. Para todo entero a, b, c se cumple:

$$a \leq b \rightarrow a + c \leq b + c$$

$$c > 0 \wedge a \leq b \rightarrow ac \leq bc$$

$$c < 0 \wedge a \leq b \rightarrow ac \geq bc$$

Los números enteros mayores que cero se denominan enteros positivos y los menores que cero se denominan enteros negativos.

10.2. Aritmética.

10.2.1. Adición. La suma de dos enteros $[m, n]$ y $[p, q]$ está definida por:

$$[m, n] + [p, q] = [m + p, n + q]$$

La adición tiene las siguientes propiedades:

- Asociativa: $(a + b) + c = a + (b + c)$
- Conmutativa: $a + b = b + a$
- Opuesto: $a + (-a) = 0$
- Neutro: $a + 0 = a$.

Las demostraciones se dejan como ejercicio.

10.2.2. Sustracción. La sustracción es una operación identificada con el símbolo $-$ $(- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z})$ definida por:

$$a - b = a + (-b)$$

El resultado de esta operación se llama *diferencia*.

10.2.3. Multiplicación. El producto de dos enteros $[m, n]$ y $[p, q]$ está definido por:

$$[m, n] \cdot [p, q] = [mp + nq, np + mq]$$

Con frecuencia, se omite el símbolo de multiplicación, y se escribe ab en lugar de $a \cdot b$.

La multiplicación tiene las siguientes propiedades:

- Asociativa: $(ab)c = a(bc)$
- Conmutativa: $ab = ba$
- Neutro: $a \cdot 1 = a$
- Cancelación: $a \cdot 0 = 0$
- Distributiva: $a(b + c) = ab + ac$

Las demostraciones se dejan como ejercicio.

10.2.4. División con resto. Dados dos enteros a, b con $b \neq 0$, siempre se pueden conseguir dos enteros q y r tales que

$$a = bq + r$$

con

$$0 \leq r \leq |q|$$

donde en este caso $|q|$ representa el valor absoluto de q y está definido por

$$|q| = \begin{cases} q & \text{si } q \geq 0 \\ -q & \text{si } q < 0 \end{cases}$$

q recibe el nombre de cociente y r resto. Los números q y r son determinados por a y b.

La operación que produce q a partir de a y b se denomina *división entera* y se suele denotar $a \div b$

La operación que produce r a partir de a y b se denomina *módulo* y se denota $a \mod b$.

Un entero a es *par* si $a \mod 2 = 0$ y es *impar* si $a \mod 2 = 1$.

10.3. Cardinalidad. La cardinalidad de $\mathbb{Z}$ es la misma de $\mathbb{N}$. Es fácil ver que la secuencia de enteros $0, 1, -1, 2, -2, 3, -3, 4, -4, \cdots$ está en biyección con los naturales.

11. NÚMEROS RACIONALES

La definición de los números racionales tiene las mismas motivaciones que la definición de los números enteros. En este caso, se agrega la posibilidad de realizar la operación de división entre dos números cualesquiera (excepto el cero).

Definición 11.1. Sea $\mathbb{Z}^*$ el conjunto de los enteros distintos de cero. Formalmente, $\mathbb{Z}^* = \mathbb{Z} - \{0\}$.

Definición 11.2. Sea $\mathcal{Q}$ la siguiente relación de equivalencia en el conjunto $\mathbb{Z}\times\mathbb{Z}^*$tal que $(m,n)\mathcal{Q}(p,q)$ si $mq = np$.

Formalmente,

$$\mathcal{Q} = \{((m,n),(p,q)) \in (\mathbb{Z}\times\mathbb{Z}^*)\times(\mathbb{Z}\times\mathbb{Z}^*) \mid mq = np\}$$

El conjunto de los números racionales es el conjunto cociente de la relación $\mathcal{Q}$ y se denota con el símbolo $\mathbb{Q}$. Formalmente,

$$\mathbb{Q} = \mathbb{Z}\times\mathbb{Z}^*/\mathcal{Q}$$

Cada clase de equivalencia de la relación $\mathcal{Q}$ es un número racional y cada elemento de $\mathbb{Z}\times\mathbb{Z}^*$ es una fracción. Una fracción (m,n) se suele representar con la notación m/n o $\frac{m}{n}$. La primera componente recibe el nombre de numerador y la segunda denominador.

Bajo la relación de equivalencia $\mathcal{Q}$ tenemos que $(1,4)$, $(2,8)$ y $(8,32)$ pertenecen a la misma clase de equivalencia. Para representar a un número racional normalmente se escoge como representante de la clase la fracción no reducible con denominador positivo. Cuando en la fracción m/n, n es 1 se suele utilizar el entero m para identificar al número racional correspondiente.

Todo racional $\frac{a}{b}$ tiene un opuesto $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$ y, si $a \neq 0$, un inverso $\frac{b}{a}$.

11.1. Aritmética.

11.1.1. Adición. La adición es una operación binaria identificada con el símbolo $+$ ($+ : \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}$) definida por:

$$\frac{m}{n} + \frac{p}{q} = \frac{mq+np}{nq}$$

La adición tiene las siguientes propiedades:

- Asociativa: $(a+b)+c = a+(b+c)$
- Conmutativa: $a+b = b+a$
- Opuesto: $a+(-a) = 0$
- Neutro: $a+0 = a$.

11.1.2. Sustracción. La sustracción es una operación identificada con el símbolo $-$ ($- : \mathbb{Q}\times\mathbb{Q} \longrightarrow \mathbb{Q}$) definida por:

$$a - b = a + (-b)$$

11.1.3. Multiplicación. La multiplicación es una operación binaria identificada con el símbolo $\cdot$ ($\cdot : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$) y definida por:

$$\frac{m}{n} \cdot \frac{p}{q} = \frac{mp}{nq}$$

Con frecuencia, se omite el símbolo de multiplicación, y se escribe ab en lugar de $a \cdot b$ ($a, b \in \mathbb{Q}$).

La multiplicación tiene las siguientes propiedades:

- Asociativa: $(ab)c = a(bc)$
- Conmutativa: $ab = ba$
- Distributiva: $a(b + c) = ab + ac$
- Neutro: $a \cdot 1 = a$
- Cancelación: $a \cdot 0 = 0$
- Inverso: $\frac{m}{n}\frac{n}{m} = 1$

11.1.4. División. La existencia del inverso permite la operación de división para todo racional (excepto con el cero). La división es una "operación binaria" identificada con el símbolo / (/ : $\mathbb{Q} \times (\mathbb{Q} - \{0\}) \longrightarrow \mathbb{Q}$) y definida por:

$$\frac{m}{n} / \frac{p}{q} = \frac{m}{n} \cdot \frac{q}{p} = \frac{mq}{np}$$

11.2. Orden. Para los números racionales se define la relación de orden estricto $<$ como:

$$\frac{m}{n} < \frac{p}{q}$$

si $mq < np$ y $nq > 0$ o si $mq > np$ y $nq < 0$.

Para dos racionales, r y s, $r \leq s \leftrightarrow r < s \vee r = s$.

$\leq$ es una relación de orden total, pero no es un buen orden. Las demostraciones se dejan como ejercicio.

El orden en los racionales es compatible con las operaciones aritméticas. Para todo racional a, b, c se cumple:

$$a \leq b \rightarrow a + c \leq b + c$$

$$c > 0 \wedge a \leq b \rightarrow ac \leq bc$$

$$c < 0 \wedge a \leq b \rightarrow ac \geq bc$$

El orden de los racionales es *denso*. Esto significa que para todos los racionales a, b tales que $a < b$ existe un racional c tal que $a < c < b$. En el caso de los racionales, si $a < b$, el número $\frac{a+b}{2}$ siempre cumple la propiedad $a < \frac{a+b}{2} < b$.

11.3. Cardinalidad. La cardinalidad de los números racionales es igual a la de los naturales ($\aleph_0$).

Es facil enumerar los racionales: $0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, \frac{1}{3}, -\frac{1}{3}, 3, -3, \frac{1}{4}, -\frac{1}{4}, \frac{2}{3}, -\frac{2}{3}, \frac{3}{2}, -\frac{3}{2}, 4, -4, \cdots$

Nótese que primero se presentan las fracciones tales que la suma del numerador y el denominador es 1, luego cuando suma 2, luego 3, etc., alternando los signos .

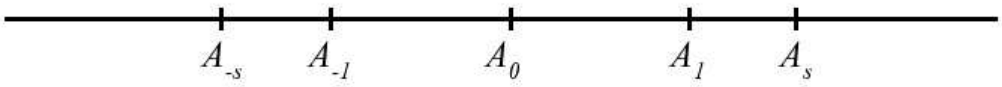


FIGURA 12.1. Representación de racionales en una recta

12. NÚMEROS REALES

12.1. Representación de racionales en una recta. En muchas áreas de la matemática es conveniente hacer uso de figuras geométricas para mostrar con mayor claridad los conceptos. Asumiendo que conocemos lo que significa una *recta*, un *segmento de recta* y la *longitud* de un segmento, consideremos una recta Λ que se extiende infinitamente en ambas direcciones.

Consideremos un segmento A_0A_1 de cualquier longitud. Nos referiremos a A_0 como el origen, o el *punto* 0 y a A_1 como el *punto* 1 y consideremos estos puntos como los números 0 y 1. Para obtener un punto que represente un racional positivo r escogemos el punto A_r tal que $A_0A_r/A_0A_1 = r$, siendo A_0A_r un segmento que va en la misma dirección de A_0A_1.

Para representar un número negativo $r = -s$, es natural designar la longitud como una magnitud con signo, positiva si la longitud se mide en la dirección A_0A_1 y negativa en la otra dirección, tal que $AB = -BA$ y que el punto A_{-s} cumpla con $A_0A_{-s} = -A_{-s}A_0 = -A_0A_s$.

De este modo obtenemos un punto A_r en la recta que corresponde a cada número racional r tal que

$$A_0A_r = r \cdot A_0A_1$$

y si tomamos A_0A_1 como nuestra unidad de medida y escribimos $A_0A_1 = 1$, tenemos $A_0A_r = r$.

Nótese que el hecho de que el orden de los racionales sea denso hace que dado un segmento BC en la recta Λ podemos encontrar tantos puntos racionales como queramos entre B y C.

Dadas estas consideraciones, podría pensarse que la recta Λ está formada únicamente por los puntos correspondientes a los racionales en dicha recta. Esta concepción, sin embargo, está errada. Un segmento de recta está formado por todos los puntos de la recta que están entre los extremos del segmento. Todo segmento tiene asociada una longitud, la cual debe ser una cantidad capaz de tener una medida numérica en términos de una unidad de longitud, y estas longitudes deben ser capaces de combinarse unas con otras mediante las operaciones de suma y multiplicación. Existen construcciones geométricas que producen longitudes que no pueden ser representadas con números racionales. Un ejemplo es la hipotenusa de un triángulo rectángulo en el que cada cateto tiene longitud 1. En este caso, la longitud x de la hipotenusa debe satisfacer, por el teorema de pitágoras, la ecuación $x^2 = 2$.

Theorem 12.1. *El número x tal que $x^2 = 2$ no puede ser un número racional.*

Demostración. Supongamos que $x = m/n$ con m y n primos entre sí. Entonces $nx = m$ y $n^2x^2 = m^2$, así que $2n^2 = m^2$. Por lo tanto m^2 es par, lo cual implica que m es par. Si m es par, entonces $m = 2k$ ($k \in \mathbb{Z}$) y $2n^2 = 4k^2$, lo cual equivale a $n^2 = 2k^2$ y por lo tanto n es par. Si m y n son ambos pares entonces no son primos entre sí, lo cual es una contradicción. □

Ejercicio. Demostrar que no existen números racionales tales que su cuadrado sea un racional m/n (m y n primos entre sí) a menos que m y n sean cuadrados perfectos.

Consideremos la ecuación $x^2 = 2$. Ya sabemos que no existe ningún racional x que satisfaga esa ecuación. Sí sabemos que el cuadrado de cualquier número racional es menor que 2 o mayor que

2. Podemos, por lo tanto, dividir los números racionales positivos (por ahora) en dos conjuntos, uno que contiene los números cuyos cuadrados son menores que 2 y el otro contiene los racionales cuyos cuadrados son mayores que 2. Llamaremos a estos dos conjuntos I, o conjunto de la izquierda y D, o conjunto de la derecha. Es obvio que todo miembro de D es mayor que todo miembro de I. Es fácil ver que siempre podremos encontrar un miembro en I cuyo cuadrado, a pesar de ser menor que 2, difiere de 2 tan poco como queramos. Por ejemplo, los cuadrados de los números $1; 1,4; 1,41; 1,414; 1,4142, \cdots$ son $1; 1,96; 1,9881; 1,999396; 1,99996164, \cdots$, los cuales son todos menores que 2, pero se aproximan tanto como deseemos.

Igualmente, siempre podremos encontrar un miembro en D cuyo cuadrado, a pesar de ser mayor que 2, difiere de 2 tan poco como queramos. Por ejemplo, los cuadrados de los números $2; 1,5; 1,42; 1,415; 1,4143; \cdots$ son $4; 2,25; 2,0164; 2,002225; 2,00024449; \cdots$, los cuales son todos mayores que 2, pero se aproximan tanto como deseemos.

También vemos que no hay un máximo elemento en I ni un mínimo elemento en D. Si x es un elemento de I, entonces $x^2 < 2$. Supongamos que $x^2 = 2 - \delta$. Siempre podemos encontrar un miembro x_1 de L tal que x_1^2 difiere de 2 en menos de δ y así $x_1^2 > x^2$ o $x_1 > x$.

Nuestra noción de sentido común sobre los atributos de una recta nos dice que debería existir un número x mayor que todos los miembros de I y menor que todos los miembros de D y un punto P en la recta tal que P divide los puntos que corresponden a los elementos de I de aquellos que corresponden a los elementos de D.

Supongamos que existe ese número x y que se puede operar con él utilizando operaciones aritméticas. Entonces x^2 no puede ser ni menor ni mayor que 2. Supongamos, por ejemplo, que $x^2 < 2$; entonces podemos encontrar un racional ξ tal que ξ^2 está entre x^2 y 2. Esto es, podemos encontrar un miembro de I mayor que x, lo cual contradice la suposición de que x divide a los elementos de I de los de D. Similarmente, x no puede ser mayor que 2. Llegamos entonces a la conclusión de que x es el número denotado por $\sqrt{2}$, el cual no es racional, ya que el cuadrado de ningún racional es 2. Este es el ejemplo más simple de lo que se conoce como un número *irracional*.

12.2. Definición de los números reales.

Definición 12.2. Un número real es un par ordenado (I, D) con las siguientes características:

1. $I \neq \emptyset$
2. $D \neq \emptyset$
3. $I \cup D = \mathbb{Q}$
4. $I \cap D = \emptyset$
5. $d \in D \wedge i \in I \rightarrow d > i$
6. I no tiene máximo elemento

Cuando D tiene un mínimo elemento, entonces el número real (I, D) corresponde a un número racional.

Cuando D no tiene mínimo entonces el número real (I, D) es un *número irracional*.

El conjunto de los números reales se denota con la letra $\mathbb{R}$.

Ejemplos:

- El número real cero (0) se puede definir como (I, D) con $I = \{x \in \mathbb{Q} \mid x < 0\}$ y $D = \{x \in \mathbb{Q} \mid x \geq 0\}$
- El número real 1 se puede definir como (I, D) con $I = \{x \in \mathbb{Q} \mid x < 1\}$ y $D = \{x \in \mathbb{Q} \mid x \geq 1\}$

- El número real -1 se puede definir como (I, D) con $I = \{x \in \mathbb{Q} \mid x < -1\}$ y $D = \{x \in \mathbb{Q} \mid x \geq -1\}$
- El número real $\sqrt{2}$ se puede definir como (I, D) con $I = \{x \in \mathbb{Q} \mid x^2 < 2 \vee x < 0\}$ y $D = \{x \in \mathbb{Q} \mid x^2 > 2 \wedge x > 0\}$

Definición 12.3. Un número real (I, D) es positivo si se cumple $\forall d(d \in D \to d > 0)$ y es negativo si no es positivo y es distinto de cero.

Definición 12.4. Todo número real $a = (I, D)$ tiene un opuesto $-a = (-D, -I)$ donde

$$-D = \begin{cases} \{-x \mid x \in D\} - \{-\text{mín}(D)\} & \text{si } D \text{ tiene mínimo} \\ \{-x \mid x \in D\} & \text{de otro modo} \end{cases}$$

$$-I = \begin{cases} \{-x \mid x \in I\} \cup \{-\text{mín}(D)\} & \text{si } D \text{ tiene mínimo} \\ \{-x \mid x \in I\} & \text{de otro modo} \end{cases}$$

Siempre se cumple que $-(-a) = a$.

Definición 12.5. Para todo número real $a \neq 0$, uno de los números a y $-a$ es positivo. El positivo lo denotamos $|a|$ y lo llamamos *valor absoluto* de a. En el caso de $a = 0$ se tiene que $|0| = 0$.

12.3. Aritmética.

12.3.1. Adición. La suma (I_c, D_c) de dos números reales (I_a, D_a) y (I_b, D_b) se define de la siguiente manera:

I_c es el conjunto formado por todas las sumas entre los elementos (racionales) de I_a e I_b. Formalmente,

$$I_c = \{x + y \mid x \in I_a \wedge y \in I_b\}$$

D_c es el conjunto de los racionales que no pertenecen a I_c y está formado por todas las sumas entre los elementos de D_a y D_b. Formalmente,

$$D_c = \mathbb{Q} - I_c = \{x + y \mid x \in D_a \wedge y \in D_b\}$$

La adición de números reales tiene las propiedades habituales presentes en la adición de racionales.

12.3.2. Sustracción. La sustracción de dos reales a y b se define por la ecuación:

$$a - b = a + (-b)$$

12.3.3. Multiplicación. En primer lugar definiremos la multiplicación de números positivos. Si $a = (I_a, D_a)$ y $b = (I_b, D_b)$ son reales positivos entonces el producto $c = (I_c, D_c)$ de a y b está definido por:

I_c es el conjunto formado por todos los productos entre los elementos de I_a e I_b. Formalmente,

$$I_c = \{xy \mid x \in I_a \wedge y \in I_b\}$$

D_c es el conjunto formado por todos los productos entre los elementos de D_a y D_b. Formalmente,

$$D_c = \mathbb{Q} - I_c = \{xy \mid x \in D_a \wedge y \in D_b\}$$

Para incluir los números negativos en la definición establecemos que si a y b son reales positivos entonces:

$$(-a)b = -ab,\ a(-b) = -ab,\ (-a)(-b) = ab$$

Finalmente, incluimos el cero en la definición estableciendo que $a(0) = (0)a = 0$ para todo real a.

12.3.4. División. Antes de definir la división debemos definir el inverso $1/a$ de un número real a ($a \neq 0$).

En primer lugar definiremos el inverso de un número real positivo $a = (I_a, D_a)$ como el par (I_b, D_b) tal que:

I_b está constituido por todos los racionales no positivos y todos los inversos de los racionales en D_a, excepto $\min(D_a)$ en caso de que D_a tenga mínimo. Formalmente,

$$I_b = \{x \in \mathbb{Q} \mid x \leq 0\} \cup \{1/x \mid x \in D_a \wedge \exists y \in D_a(y < x)\}$$

D_b está constituido por todos los racionales que no pertenecen a I_b, es decir, todos los inversos de los racionales positivos en I_a y el inverso del mínimo de D_a en caso de que lo haya. Formalmente,

$$D_b = \mathbb{Q} - I_a = \{1/x \mid x \in I_a \wedge x > 0\} \cup \{1/x \mid x \in D_a \wedge \forall y \in D_a(x \leq y)\}$$

El inverso de un número negativo $-a$ lo definimos con la ecuación $1/(-a) = -(1/a)$.

Finalmente definimos el cociente de los reales a y b como $a/b = a \cdot (1/b)$.

12.4. Orden. Sean dos números reales $a = (I_a, D_a)$ y $b = (I_b, D_b)$. Siempre se cumple que $I_a \subseteq I_b \vee D_a \subseteq D_b$.

Definición 12.6. Una relación de orden total y denso en $\mathbb{R}$ es $(I_a, D_a) \leq (I_b, D_b) \leftrightarrow I_a \subseteq I_b$.

Siempre se cumple uno y sólo uno de los siguientes casos (tricotomía):

1. $I_a \subseteq I_b \wedge D_a \subseteq D_b \leftrightarrow a = b$
2. $I_a \subseteq I_b \wedge D_a \nsubseteq D_b \leftrightarrow a < b$
3. $D_a \subseteq D_b \wedge I_a \nsubseteq I_b \leftrightarrow a > b$

La Figura 12.2 facilita el entendimiento de estos tres casos.

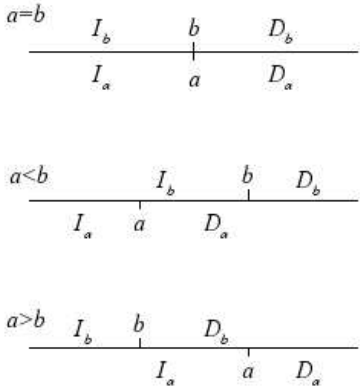


FIGURA 12.2. Tricotomía en los reales

El orden en los reales es compatible con las operaciones aritméticas.

El conjunto de los números reales es *completo* ya que todo subconjunto no vacío con una cota superior tiene supremo.

12.5. Expansión decimal. Todo número real a tiene una expansión decimal

$$x = n + 0, d_1 d_2 d_3 ...$$

donde n es un entero y cada d_i es un dígito entre 0 y 9 y la secuencia de dígitos no termina con un número infinito de 9s consecutivos. Esta representación significa lo siguiente:

$$n + \frac{d_1}{10} + \frac{d_2}{100} + \cdots + \frac{d_k}{10^k} \leq x < n + \frac{d_1}{10} + \frac{d_2}{100} + \cdots + \frac{d_k}{10^k} + \frac{1}{10^k}$$

12.6. Cardinalidad. Los números reales no son enumerables. A continuación una demostración que muestra que el conjunto $\{r \in \mathbb{R} \mid 0 < r < 1\}$ no es enumerable.

Demostración. Asumamos que el conjunto es enumerable. Entonces podemos listar todos los números del conjunto como una secuencia $r_1, r_2, r_3, \cdots$. Construiremos un número real z entre 0 y 1 como sigue:

- Si el n-simo dígito de la parte fraccionaria de la expansión decimal de r_n es 0, entonces el n-simo dígito de z es 1.
- Si el n-simo dígito de la parte fraccionaria de la expansión decimal de r_n es distinto de 0, entonces el n-simo dígito de z es 0.

z es claramente un número real pero es imposible que esté en la secuencia, ya que su n-simo dígito difiere del n-simo dígito de r_n.

Por ejemplo, si la lista es:

$$\begin{aligned} r_1 &= 0,0123176... \\ r_2 &= 0,4147656... \\ r_3 &= 0,8242782... \\ r_4 &= 0,2330331... \\ r_5 &= 0,7676142... \\ r_6 &= 0,5490901... \\ &\vdots \end{aligned}$$

Entonces z es $0,100101...$ y es claramente un real que no está en la lista. □

La cardinalidad de los números reales se denota c y se denomina *continuo*. $c = \mathcal{P}(\aleph_0)$ y es igual a la cardinalidad del conjunto de todos los subconjuntos de números naturales.

La cardinalidad de los puntos de un segmento de recta es igual a la de todos los puntos de una recta y es igual a la de los puntos en un plano, un cubo o una circunferencia.

13. Números Complejos

Los números reales pueden ser generalizados de varias maneras, aunque ninguna permite conservar todas las propiedades. La generalización más común la constituyen los números complejos.

Definición 13.1. Un número complejo z es un par ordenado (x, y) donde $x, y \in \mathbb{R}$.

El conjunto de los números complejos se denota con la letra $\mathbb{C}$.

El número real a corresponde al número complejo $(a, 0)$. En particular, el número real 1 corresponde al complejo $(1, 0)$

Normalmente, el número complejo $(0, 1)$ se conoce como *unidad imaginaria* y se denota con la letra i.

Un número complejo (x, y) se representa normalmente como $x + iy$. $(x, y) = (1, 0)x + (0, 1)y = x + iy$.

Definición 13.2. Si $z = x + iy$ es un complejo, entonces el número real $\Re(z) = x$ se denomina *parte real* de z y el número real $\Im(z) = y$ se denomina *parte imaginaria* de z.

13.1. Aritmética. La aritmética de los complejos está definida de manera tal que las operaciones sean análogas a las correspondientes a los números reales, pero estableciendo que $i^2 = -1$.

13.1.1. Adición. La suma de dos complejos $a + bi$ y $c + di$ está definida como:

$$(a + bi) + (c + di) = (a + c) + i(b + d)$$

13.1.2. Sustracción. La diferencia de dos complejos $a + bi$ y $c + di$ está definida como:

$$(a + bi) - (c + di) = (a - c) + i(b - d)$$

13.1.3. Multiplicación. El producto de dos complejos $a + bi$ y $c + di$ está definido como:

$$(a + bi)(c + di) = (ac - bd) + i(ad + bc)$$

13.1.4. División. El cociente de dos complejos $a + bi$ y $c + di$ está definido como:

$$\frac{a + bi}{c + di} = \frac{(ac + bd) + i(bc - ad)}{c^2 + d^2}$$

13.2. Representación geométrica. Un número complejo puede verse como un desplazamiento en un sistema de coordenadas cartesiano de dos dimensiones (ver Figura 13.1).

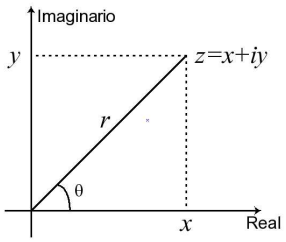


FIGURA 13.1. Representación geométrica de un número complejo $z = x + iy$

En la Figura 13.1 puede observarse que el número complejo forma un triángulo rectángulo con hipotenusa r y catetos x y y.

Está claro que $x = r\cos\theta$ y $y = r\,\mathrm{sen}\,\theta$ y por lo tanto $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$. Se puede demostrar mediante expansión en serie de potencias que $e^{i\theta} = \cos\theta + i\,\mathrm{sen}\,\theta$ y por lo tanto podemos escribir $z = re^{i\theta}$. Esta notación facilita las operaciones de multiplicación y división de complejos.

En el caso de la multiplicación, si $z_1 = r_1e^{i\theta_1}$ y $z_2 = r_2e^{i\theta_2}$ entonces $z_1z_2 = r_1r_2e^{i(\theta_1+\theta_2)}$.

En el caso de la división, si $z_1 = r_1e^{i\theta_1}$ y $z_2 = r_2e^{i\theta_2}$ entonces $\frac{z_1}{z_2} = \frac{r_1}{r_2}e^{i(\theta_1-\theta_2)}$.

La notación $z = re^{i\theta}$ da lugar a la ecuación $e^{i\pi} + 1 = 0$, que relaciona los cinco números fundamentales de la matemática.

Definición 13.3. El número real $r = \sqrt{x^2 + y^2}$ se denomina *valor absoluto* o *norma* de z y se denota $|z|$ y el número real θ se denomina *argumento* de z.

Definición 13.4. Si $z = x + iy$, el número complejo $x + i(-y) = x - iy$ se denomina *conjugado* de z y se denota $\overline{z}$.

Theorem 13.5. *A continuación algunas propiedades del conjugado:*

1. $\overline{\overline{z}} = z$
2. $\overline{z + w} = \overline{z} + \overline{w}$
3. $\bar{z} = z \leftrightarrow y = 0$
4. $|z| = |\bar{z}|$
5. $|z|^2 = z\bar{z}$
6. $1/z = \bar{z}/\left|z\right|^2$

Demostración. Ejercicio. □

13.3. Algunas propiedades.

13.3.1. Orden. A diferencia de los reales, los complejos no se pueden ordenar de ninguna manera que sea compatible con las operaciones aritméticas.

Supongamos que $i > 0$, entonces multiplicando por i nos queda $i^2 > 0$, lo cual equivale a $-1 > 0$ lo cual es falso.

Supongamos que $i < 0$, entonces $0 < -i$, multiplicando por $-i$ nos queda $0 < (-i)^2 = i^2 = -1$ lo cual es falso.

Entonces la unidad imaginaria no es comparable con el cero .

13.3.2. Teorema fundamental del álgebra. Todo polinomio de grado n tiene n raíces complejas (contando las raíces con su orden de multiplicidad). Es decir, si $p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + z^n$ donde $a_0, a_1, ..., a_{n-1}$ son números reales o complejos, entonces existen números complejos (no necesariamente diferentes) $z_1, z_2, ..., z_n$ tales que $p(z) = (z - z_1)(z - z_2)\cdots(z - z_n)$.

REFERENCIAS

[1] Allard, W. *The Rational Numbers*. Duke University. 2004.
[2] Allard, W. *Sets, relations and functions*. Duke University. 2004.
[3] Brown, C. *Set Theory Handout*. Trinity University. 2004.
[4] Halmos. *Naive Set Theory*. D. Van Nostran Company, Inc. 1960.
[5] Hardy, G. H. *A Course of Pure Mathematics*. Cambridge University Press. 2000.
[6] Johnsonbaugh, R. *Matemáticas Discretas*. Prentice Hall Hispanoamericana. 1999.
[7] Knuth, D. E. *The Art of Computer Programming. Volume 1. Fundamental Algorithms*. Addison Wesley Longman. 1998.
[8] Lewin, R. *Teoría Axiomática de Conjuntos*. Pontificia Universidad Católica de Chile. 2004.
[9] Mathematical Institute. *Lecture Notes and Problem Sheets*. University of Oxford. 2004.
[10] MathWorld. *Complex number*. http://www.mathworld.wolfram.com
[11] MathWorld. *Real number*. http://www.mathworld.wolfram.com
[12] Velleman, Daniel. *How To Prove It*. Cambridge University Press. 1994.
[13] Wikipedia. *Canthor's diagonal argument*. http://www.wikipedia.org
[14] Wikipedia. *Canthor's theorem*. http://www.wikipedia.org
[15] Wikipedia. *Complex number*. http://www.wikipedia.org
[16] Wikipedia. *Countable set*. http://www.wikipedia.org
[17] Wikipedia. *Fundamental theorem of algebra*. http://www.wikipedia.org
[18] Wikipedia. *Mathematical induction*. http://www.wikipedia.org
[19] Wikipedia. *Naive Set Theory*. http://www.wikipedia.org
[20] Wikipedia. *Peano axioms*. http://www.wikipedia.org

[21] Wikipedia. *Proof of mathematical induction*. http://www.wikipedia.org
[22] Wikipedia. *Real numbers*. http://www.wikipedia.org